Montana Operations Manual ***POLICY***	Category	**Security**
	Effective Date	
	Last Revised	
Issuing Authority	**Department of Administration** **State Information Technology Services Division**	
POL–Information Security Policy		

I. Purpose

This Policy outlines the requirements for information technology security risk management.

II. Scope

This Policy applies to all executive branch agencies and independent contractors, excluding the university system, who have access to, use, or manage state government-controlled information systems.

III. Policy Statement

A. General

Agencies shall use the National Institute of Standards and Technology (NIST) publications as guidance in information technology security risk management.

B. Security Risk Management Programs

Agencies shall construct and maintain information technology security risk management programs using the NIST Special Publication 800-39 framework and Federal Information Processing Standards Publications 199 and 200 as guidance.

C. Risk Management Control Set

The state has established guidance with respect to baseline security controls, which are consistent with NIST Moderate systems. These controls are located in POL-Information Security Policy Appendix A - Baseline Security Controls – State of Montana. Agencies may implement additional controls beyond listed controls. Agencies will evaluate and categorize information systems as part of their respective information security management programs to determine appropriate baseline controls based on the criticality and sensitivity of the information managed by each system. Baseline controls should be evaluated as part of a risk-based security process and tailored POL-Information Technology Security Risk Management Policy appropriately to achieve cost-effective, risk-based security that supports agency mission/business needs.

D. Roles and Responsibilities

POL-Information Security Policy Appendix B - Security Roles and Responsibilities is provided as a guide for the roles and responsibilities structure recommended for State of Montana Information Security Program management. At a minimum each department head is responsible for ensuring an adequate level of security for all data within that department and shall designate an Information Security Manager (ISM) to administer the department's security program for data (MCA 2-15-114, Security responsibilities of departments for data).

E. Cybersecurity Framework Core

Framework Core Functions:

1. IDENTIFY
   - Asset Management
   - Business Environment
   - Governance
   - Risk Assessment
   - Risk Management Strategy
2. PROTECT
   - Access Control
   - Awareness and Training
   - Data Security
   - Information Protection Processes and Procedures
   - Maintenance
   - Protective Technology
3. DETECT
   - Anomalies and Events
   - Security Continuous Monitoring
   - Detection Processes
4. RESPOND
   - Response Planning
   - Communications
   - Analysis
   - Mitigation
   - Improvements
5. RECOVER
   - Recovery Planning
   - Improvements
   - Communications

All agencies, staff and all others, including outsourced third-parties (such as contractors, or other service providers), who have access to, or use or manage information assets subject to the policy and standard provisions of §2-17-534, MCA shall:

1. <u>IDENTIFY</u>

1.1. Maintain an inventory of information system components. Inventory of systems is conducted annually and reviewed for any unauthorized components. Unauthorized components are removed.

1.2. Map organizational communication and data flows by:

1.2.1. Approving flow of information between information systems;

1.2.2. Requiring an Interconnection Security Agreement for all information systems directly connected to external systems;

1.2.3. Outlining connections with other information systems within the system security plan;

1.2.4. Employing a permit-by documented request (exception) policy for allowing agency and other information systems to connect to external information system; and

1.2.5. Ensuring that all internal connections for an information system are documented within the system security plan.

1.3. Maintain agreements with external entities when using external information systems to use, process, store, or transmit state data that includes the following:

1.3.1. Ensuring compliance with access requirements;

1.3.2. Requiring that providers of external information system services comply with organizational information security requirements and employ appropriate security in accordance with applicable state laws, Executive Orders, policies, standards, and guidance;

1.3.3. Defining and documenting State of Montana oversight and user roles and responsibilities with regard to external information systems;

1.3.4. Monitoring security control compliance by external service providers; and

1.3.5. Requiring providers of information system services to identify the functions, ports, protocols, and other services required for the use of such services.

1.4. Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners).

1.5. Establish dependencies, critical functions, and requirements, for delivery of critical services.

1.6. Establish and maintain information security policies that provide the following:

1.6.1. Coordination and alignment of information security roles and responsibilities with internal roles and external partners;

1.6.2. Ensure that legal and regulatory requirements regarding information security, including privacy and civil liberties obligations, are understood and managed; and

1.6.3. Ensure governance and risk management processes address information security risks.

1.7. Identify and document asset vulnerabilities by:

1.7.1. Obtaining, protecting as required, and making available to authorized personnel, administrator documentation for the information system that describes:

1.7.1.1. Secure configuration, installation, and operation of the information system;

1.7.1.2. Effective use and maintenance of security features/functions; and

1.7.1.3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

1.7.2. Obtaining, protecting as required, and making available to authorized personnel, user documentation for the information system that describes:

1.7.2.1. User-accessible security features/functions and how to effectively use those security features/functions;

1.7.2.2. Methods for user interaction with the information system, which enables individuals to use the system a more secure manner; and

1.7.2.3. User responsibilities in maintaining the security of the information and information system.

1.7.3. Documenting attempts to obtain information system documentation when such documentation is either unavailable or nonexistent;

1.7.4. Protecting documentation as required in accordance with the risk management strategy;

1.7.5. Scanning for vulnerabilities in information systems and hosted applications annually and when new vulnerabilities potentially affect the system/applications are identified and reported;

1.7.6. Employing vulnerability scanning tools and techniques that promote interoperability among tools and automating parts of the vulnerability management process by using standards for:

1.7.6.1. Enumerating platforms, software flaws, and improper configurations;

1.7.6.2. Formatting and making transparent, checklists and test procedures; and;

1.7.6.3. Measuring vulnerability impact;

1.7.7. Analyzing vulnerability scan reports and results from security control assessments;

1.7.8. Remediating critical vulnerabilities within thirty (30) business days in accordance with an organizational assessment of risk;

1.7.9. Sharing information obtained from the vulnerability scanning process and security control assessments with designated personnel to help eliminate similar vulnerabilities in other information systems;

1.7.10. Employing a vulnerability scanning tool that automates vulnerability list updates at least weekly, prior to a new scan, and when new vulnerabilities are identified and reported;

1.7.11. Authorizing privileged access for vulnerability scanning activities;

1.7.12. Requiring that information system developers/integrators:

1.7.12.1. Create and implement a security test and evaluation plan;

1.7.12.2. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process;

1.7.12.3. Document the results of the security testing/evaluation and flaw remediation processes.

1.8. Receive security alerts, advisories, and directives that:

1.8.1. Originate from designated trusted external organizations;

1.8.2. Are communicated on an ongoing basis;

1.8.3. Generate internal security alerts, advisories, and directives as deemed necessary;

1.8.4. Are disseminated to appropriate entity/agency security contracts for their use and distribution;

1.8.5. Are used to implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance;

1.8.6. Are used to facilitate ongoing security education and training for organizational personnel;

1.8.7. Assist with maintaining currency with recommended security practices, techniques, and technologies;

1.8.8. Include current threats, vulnerabilities, and incidents; and

1.8.9. Are used to implement a threat awareness program that includes a cross-organization information-sharing capability.

1.9. Conduct risk assessments that include the following:

1.9.1. The likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and the information it processes, stores, or transmits;

1.9.2. Documentation of the risk assessment results in a risk assessment report;

1.9.3. Annual review of the risk assessment results; and

1.9.4. Annual updates or whenever there are significant changes to information systems or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may affect the security state of the system.

1.10. Establishes security categorizations that:

1.10.1. Are in accordance with applicable state laws, Executive Orders, directives, policies, standards, and guidance;

1.10.2. Are documented within the security plan for each information system; and

1.10.3. Ensures the authorizing official or designated representative reviews and approves of the security categorization decision.

1.11. Implement a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are:

1.11.1. Developed and maintained;

1.11.2. Contain documentation of the remedial information actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the State; and

1.11.3. Reported in manner consistent with State of Montana (OMB FISMA) requirements.

1.12. Develop and implement a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes the following:

1.12.1. Establishing and communicating priorities for organizational mission, objectives and activities;

1.12.2. A determination of organizational risk tolerance that is clearly expressed and communicated;

1.12.3. A definition of mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the State;

1.12.4. A determination of information protection needs arising from the defined mission/business processes and revision to the processes as necessary, until an achievable set of protection needs is obtained; and

1.12.5. Development, documentation, and updating of critical infrastructure and key resources protection plan.

Back

2. **PROTECT**

2.1. Manage identities and credentials for authorized devices and users that:

2.1.1. Provides unique identification and authentication to information systems;

2.1.2. Employs the use of multifactor authentication for access to privileged accounts;

2.1.3. Provides unique identification and authentication to all network attached devices compatible with the 802.1X protocol prior to establishing a network connection;

2.1.4. Provides unique information system identifiers (UserID)s by:

2.1.4.1. Requesting the identifier from SITSD;

2.1.4.2. Receiving authorization from an authorizing manager;

2.1.4.3. Selecting an identifier that identifies an individual, group role, or device;

2.1.4.4. Assigning the identifier to the intended individual group, role, or device; and

2.1.4.5. Prohibiting the reuse of identifiers.

2.1.5. Requires the following of identifiers:

2.1.5.1. Password have a minimum of eight (8) characters that contain lower case and upper case letters and numbers;

2.1.5.2. Password must be changed upon first login;

2.1.5.3. Password changes are required every sixty (sixty) days;

2.1.5.4. Password encryption during both storage and transmission;

2.1.5.5. Password reuse is prohibited for six (6) generations; and

2.1.5.6. Follows developed agency documented provisioning and de-provisioning processes.

2.1.6. Requires that certificates are validated and map the identity to the user account;

2.1.7. Requires that hardware token-based authentication employs mechanisms that satisfy Public Key Infrastructure (PKI) requirements;

2.1.8. Obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals;

2.1.9. Employs cryptographic authentication, on systems with sensitive information, that complies with requirements set forth by applicable policies, standards, and guidance;

2.1.10. Identifies and authenticates non-organizational users using federated identify mechanisms (ePass) that allows authentication to some external platforms and services;

2.1.11. Identifies information system accounts by type e.g., individual, shared, group, system, guest/anonymous, emergency, developer, manufacturer, vendor, temporary, and service;

2.1.12. Assigns account managers for information system accounts;

2.1.13. Establishes conditions for group and role membership;

2.1.14. Specifies authorized users of the information system, group and role memberships, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

2.1.15. Requires approvals by system owners, a contract manager, or business manager for requests to create information system accounts;

2.1.16. Creates, enables, modifies, disables, and removes information system accounts in accordance with account managers;

2.1.17. Monitors the use of, information system accounts;

2.1.18. Employs automated mechanisms to support the management of information system accounts;

2.1.19. Automates the disabling of temporary and emergency accounts after sixty (60) days;

2.1.20. Automates the disabling of inactive accounts and identifiers after ninety (90) days; and

2.1.21. Automates the auditing and provides notification to account managers the following account actions:

2.1.21.1. Creation

2.1.21.2. Modification

2.1.21.3. Enabling

2.1.21.4. Disabling

2.1.21.5. Removal

2.2. Notify account managers through the information system owner when:

2.2.1. Accounts are no longer required;

2.2.2. Users are terminated or transferred; and

2.2.3. Individual information system usage or need-to-know changes.

2.3. Authorize access to information systems based on:

2.3.1. Valid access authorization;
2.3.2. Intended system usage; and

2.3.3. Other attributes as required by the mission\business function.

2.4. Manage and protect physical access to assets that:

2.4.1. Require a current list of personnel with authorized access to the facilities where information systems reside;

2.4.2. Require the issuance of authorization credentials;

2.4.3. Require the review and approval of the access list and authorization credential on a monthly basis;

2.4.4. Remove personnel from the access list that no longer require access;

2.4.5. Enforce physical access authorizations for all physical access points where the information system resides;

2.4.6. Verify individual access authorizations before granting access to facilities;

2.4.7. Control entry to facilities containing the information systems using physical access controls;

2.4.8. Control access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;

2.4.9. Secure keys, combinations, and other physical access devices;

2.4.10. Inventory physical access devices annually;

2.4.11. Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

2.4.12. Control physical access to information system distribution and transmission within state facilities;

2.4.13. Control physical access to sensitive information system output devices to prevent unauthorized individuals from obtaining the output;

2.4.14. Monitor physical access by:

2.4.14.1. Detecting and responding, in real time, to physical security incidents;

2.4.14.2. Reviewing physical access logs monthly; and

2.4.14.3. Coordinating results of reviews and investigations with the state's incident response capability.

2.4.15. Maintain visitor access records to facilities that house sensitive information systems and reviews visitor access records monthly; and

2.4.16. Protect power equipment and power cabling for sensitive information from damage and destruction.

2.5. Manage Remote Access that:

2.5.1. Maintains usage restriction, configuration requirements, and implementation guidance;

2.5.2. Requires multifactor authentication;

2.5.3. Requires authorization from the information system owner;

2.5.4. Monitors all access sessions;

2.5.5. Utilizes encryption;

2.5.6. Routes traffic through SITSD enterprise designated control points;

2.5.7. Restricts the use of privileged commands to system administrators;

2.5.8. Maintains terms and conditions for the use of mobile device to access state information systems; and

2.5.9. Requires that agreements are established with external entities when utilizing external information systems to use, process, store or transmit state data.

2.6. Manage access permissions that:

2.6.1. Incorporates the principle of least privilege according to mission and business function;

2.6.2. Incorporates and documents the principle of separation of duties; and

2.6.3. Approves access to State systems.

2.7. Protect network integrity by:

2.7.1. Approving flow of information between information systems;

2.7.2. Monitoring and controlling communications at the external boundary of the system and at key internal boundaries within the system;

2.7.3. Connecting to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with security architecture;

2.7.4. Allocating publicly accessible State of Montana network components to separate sub-network with separate physical network interfaces;

2.7.5. Preventing public access into the State of Montana’s internal networks except as appropriately mediated by managed interfaces employing boundary protection devices;

2.7.6. Limiting the number of access points to the State of Montana network to allow for more comprehensive monitoring of inbound and outbound communications and network traffic;

2.7.7. Implementing a managed interface for each external telecommunication service;

2.7.8. Establishing a traffic flow ruleset for each managed interface that denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception);

2.7.9. Employing security controls as needed to protect the confidentiality and integrity of the information being transmitted;

2.7.10. Documenting each exception to the traffic flow policy with supporting mission/business need and duration of that need;

2.7.11. Reviewing exceptions to the traffic flow ruleset annually or upon request;

2.7.12. Removing traffic flow policy exceptions that are no longer supported by an explicit mission/business need; and

2.7.13. Preventing remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

2.8. Provide State of Montana personnel and partners cybersecurity awareness education that:

2.8.1. Includes basic security awareness training to new employees prior to provisioning access to systems or performance of duties;

2.8.2. Requires annual security awareness training to all other staff members including managers, senior executives, and contractors; and

2.8.3. Requires that privileged users understand and acknowledge their roles and responsibilities

2.9. Manage information and records consistent with the organization's risk strategy to protect confidentiality, integrity, and availability that:

2.9.1. Employs appropriate security technologies for data-at-rest;

2.9.2. Employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures;

2.9.3. Requires assets are formally managed by:

2.9.3.1. Maintaining an inventory of information system components;

2.9.3.2. Conducting annual reviews of information system inventory;

2.9.3.3. Removing unauthorized components;

2.9.3.4. Sanitizing sensitive information system media (both digital and non-digital), with sanitization mechanisms that are commensurate with the classification or sensitivity of the information, prior to disposal, release of organizational control, or reuse; and

2.9.3.5. Authorizing, monitoring, and controlling servers, server racks, hard drives, workstations, network arrays, network equipment, and any other pertinent equipment entering and exiting secured data center facilities and maintaining records of those items.

2.9.4. Maintains adequate capability and capacity to ensure availability by:

2.9.4.1. Allowing flexibility in audit storage capacity; and

2.9.4.2. Protecting against or limiting the effects of denial of service attacks.

2.9.5. Protects against data leaks by:

2.9.5.1. Approving flow of information between information systems;

2.9.5.2. Documenting separation of duties;

2.9.5.3. Employing the principle of least privilege according to mission/business functions;

2.9.5.4. Screening individuals prior to authorizing access to information systems and rescreening individuals according to the following conditions:

2.9.5.4.1. Job Transfer/Hire into a position that require additional security/privileged access; and

2.9.5.4.2. Every three (3) years.

2.9.5.5. Ensuring that individuals who have access to organizational sensitive information, sign appropriate access agreements prior to being granted access;

2.9.5.6. Reviewing and updating access agreements every two (2) years;

2.9.5.7. Employing boundary protection mechanisms;

2.9.5.8. Employing cryptographic mechanisms, protections, and modules that comply with applicable state laws, Executive Orders, policies, standards and guidance;

2.9.5.9. Monitoring events by:

2.9.5.9.1. Utilizing security incident and event monitoring objectives to detect information system attacks; and

2.9.5.9.2. Identifying unauthorized use of information systems;

2.9.6. Detects unauthorized changes to software and information, and reassesses the integrity of software and information by performing integrity scans of the information system on an annual basis; and

2.9.7. Maintains separate development and testing environments along with baseline configuration for rollback support.

2.10. Create and maintain a baseline configuration of information technology systems that:

2.10.1. Requires a review bi-annually or as needed;

2.10.2. Retains older versions of baseline configurations for rollback support;

2.10.3. Employs a formal change management system that includes the following:

2.10.3.1. Types of changes that need to be documented in the tool;

2.10.3.2. Approval process that includes security review;

2.10.3.3. Documentation of approved changes;

2.10.3.4. Retention records of changes and review processes;

2.10.3.5. Auditing of change activities;

2.10.3.6. Coordination and oversight capabilities for configuration change control activities;

2.10.3.7. Capability to approve, hold until approved, and document the completion of requested changes; and

2.10.3.8. Processes to test, validate, and document changes prior to implementation.

2.10.4. Requires testing, validation, and documentation prior to implementation of changes in order to determine potential security impacts;

2.10.5. Requires review by appropriate security staff prior to change implementation;

2.10.6. Restricts physical and logical access for changes to appropriate staff;

2.10.7. Maintains mandatory configuration settings for each information system;

2.10.8. Requires approval and documentation of exceptions to mandatory settings;

2.10.9. Maintains the principle of least functionality. That is, information system functions, ports, protocols, and/or services are limited where applicable; and

2.10.10. Employs a configuration management plan.

2.11. Manage information systems using a system development lifecycle methodology that:

2.11.1. Includes information security considerations;

2.11.2. Defines and documents information system security roles and responsibilities throughout the system development lifecycle; and

2.11.3. Identifies individuals having information system security roles and responsibilities.

2.11.4. Requires information system acquisition contracts include the following:

2.11.4.1. Security functional requirements/specifications;

2.11.4.2. Security-related documentation requirements;

2.11.4.3. Developmental and evaluation-related assurance requirements;

2.11.4.4. Functional properties of the security controls to be employed within information systems, information system components, or information system services in sufficient detail to permit analysis and testing of the controls;

2.11.4.5. Security-relevant external system interfaces and high-level design;

2.11.4.6. Identification of the functions, ports, protocols, services intended for organization use.

2.11.4.7. Information technology products are on the FIPS 201-approved product list for Personal Identify Verification (PIV).

2.11.5. Includes system security engineering principles in the specification, design, development, implementation, and modification of the information system;

2.11.6. Requires information system developers/integrators perform the following:

2.11.6.1. Configuration management during information system design, development, implementation, and operation;

2.11.6.2. Management and control changes to the information system;

2.11.6.3. Implementation of only organization-approved changes;

2.11.6.4. Documentation of approved changes to the information system;

2.11.6.5. Tracking of security flaws and flaw resolution;

2.11.6.6. Creation of a security test and evaluation plan;

2.11.6.7. Implementation of a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and

2.11.6.8. Documentation of the security testing/evaluation and flaw remediation processes.

2.11.7. Requires development of an information security architecture for the information system that:

2.11.7.1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

2.11.7.2. Describes how the information security architecture is integrated into and supports the enterprise architecture;

2.11.7.3. Describes any information security assumptions about, and dependencies on, external services;

2.11.7.4. Reviews and updates the information security architecture every two years to reflect updates in the enterprise architecture; and

2.11.7.5. Ensures that planned information security architecture changes are reflected in the operational security plan and organizational procurements/acquisitions.

2.12. Maintain a physical operating environment for state assets that:

2.12.1. Provides for the following emergency shutoff capabilities:

2.12.1.1. Shutting off power to sensitive information systems or individual system components in emergency situations;

2.12.1.2. Placement of emergency shutoff switches or devices in appropriate locations within secured facilities to facilitate safe and easy access for personnel;

2.12.1.3. Protection of emergency power shutoff capability from unauthorized activation;

2.12.2. Provides a short-term uninterruptible power supply to facilitate an orderly shutdown of information systems in the event of a primary power source loss; and

2.12.3. Employs automatic emergency lighting for information systems that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within facilities;

2.12.4. Provides for the following fire protection capabilities:

2.12.4.1. Fire suppression and detection systems for sensitive information systems that are supported by an independent energy source;

2.12.4.2. Fire detection systems for sensitive information systems that activates automatically and notifies authorized personnel and emergency responders in the event of a fire;

2.12.4.3. Fire suppression systems for sensitive information systems that provides automatic notification for any activation State emergency responders; and

2.12.4.4. Fire suppression system for sensitive information systems in unstaffed facilities.

2.12.5. Maintains temperature and humidity levels within the facilities where sensitive information resides between 68-71 degrees Fahrenheit and humidity can be anywhere from 28% to 54%; temperature and humidity levels are monitored 24/7;

2.12.6. Protects sensitive information systems from damage resulting from water leakage by ensuring a master shutoff valve is accessible, working properly, and known to key personnel; and

2.12.7. Authorizes, monitors, and controls servers, server racks, hard drives, workstations, network arrays, network equipment, and any other pertinent equipment entering and exiting secured data center facilities and maintains records of those items.

2.13. Sanitize sensitive information system media (both digital and non-digital) prior to disposal, release of organizational control, or reuse. NOTE: Employed sanitization mechanisms (strength and integrity) must be commensurate with the classification and sensitivity of the information.

2.14. Continuously improve protection processes by:

2.14.1. Creating a formal System Security Plan that:

2.14.1.1. Is consistent with the organization’s enterprise architecture;

2.14.1.2. Explicitly defines the authorization boundary for the system;

2.14.1.3. Describes the operational context of the information system in terms of mission and business processes;

2.14.1.4. Provides the security categorization of the information system including supporting rationale;

2.14.1.5. Describes the operational environment for the information system and relationships with or connections to other information systems;

2.14.1.6. Provides an overview of the security requirements for the system;

2.14.1.7. Identifies any specific statutory and/or regulatory requirements (above and beyond Moderate Baseline Controls), if applicable;

2.14.1.8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and

2.14.1.9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

2.14.2. Distributing copies of the System Security Plan and communicating changes to the plan to appropriate personnel;

2.14.3. Reviewing the System Security Plan for the information system at least once every year;

2.14.4. Updating the System Security Plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments;

2.14.5. Protecting the System Security Plan from unauthorized disclosure and modification;

2.14.6. Planning and coordinating security-related activities with other organizational entities before conducting such activities in order to reduce the impact on enterprise operations, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing.

2.14.7. Developing, monitoring, and reporting on the results of information security measures of performance.

2.14.8. Developing a continuous monitoring strategy and implementing a continuous monitoring program that:

2.14.8.1. Establishes metrics to be monitored;

2.14.8.2. Establishes frequencies for monitoring and frequencies for assessments supporting such monitoring;

2.14.8.3. Develops ongoing security control assessments in accordance with the agency continuous monitoring strategy;

2.14.8.4. Develops ongoing security status monitoring of agency-defined metrics;

2.14.8.5. Correlates and analyzes security-related information generated by assessments and monitoring;

2.14.8.6. Develops response actions to address results of the analysis of security related information;

2.14.8.7. Reports the security status of the agency and information systems to agency-defined personnel within agency-defined frequency; and

2.14.8.8. Employs assessors or assessment teams with an agency-defined level of independence to monitor the security controls in the information system on an ongoing basis.

2.14.9. Sharing the effectiveness of protection technologies with appropriate parties.

2.14.10. Ensuring that response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

2.14.11. Ensuring that response and recovery plans are tested.

2.14.12. Ensuring that cybersecurity is included in human resources practices that:

2.14.12.1. Assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions;

2.14.12.2. Reviews and revises position risk designations every two years;

2.14.12.3. Upon termination of individual employment the agency shall:

2.14.12.3.1. Terminate all information system access;

2.14.12.3.2. Conduct exit interviews;

2.14.12.3.3. Retrieve all security-related organizational information system-related property; and

2.14.12.3.4. Retain access to organizational information and information systems formerly controlled by terminated individual.

2.14.12.4. Upon reassigning or transferring agency personnel to other positions within the State, agencies shall conduct a review of logical and physical access authorizations to information systems/facilities within three business days of beginning the new position to ensure access is limited to authorized and required systems/facilities.

2.14.12.5. Establishes third-party personnel security requirements that:

2.14.12.5.1. Includes security roles and responsibilities for the providers;

2.14.12.5.2. Documents personnel security requirements; and

2.14.12.5.3. Monitors provider compliance.

2.14.12.6. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

2.14.13. Developing and implementing a vulnerability management plan.

2.15. Maintain and repair organization assets by:

2.15.1. Utilizing a formalized change management process;

2.15.2. Performing maintenance on major equipment that contains sensitive information on-site;

2.15.3. Performing security checks that are performed after maintenance is completed;

2.15.4. Approving, controlling, monitoring the use of, and maintaining on an ongoing basis, information system maintenance tools;

2.15.5. Checking information system maintenance tools prior to admittance into a secured data center facility;

2.15.6. Checking all media for virus or malicious code before it is used on an information system;

2.15.7. Establishing a process for maintenance personnel authorization by maintaining a current list of authorized maintenance organizations or personnel; and

2.15.8. Ensuring that personnel performing maintenance on an information system that contains sensitive information have had a background check.

2.16. Perform remote maintenance of organizational assets in a secure manner by:

2.16.1. Authorizing, monitoring, and controlling all non-local maintenance and diagnostic activities;

2.16.2. Allowing the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the system security plan for the information system;

2.16.3. Employing strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;

2.16.4. Maintaining records for non-local maintenance and diagnostic activities; and

2.16.5. Terminating all session and network connection when non-local maintenance is completed.

2.17. Manage information system audit/log records by:

2.17.1. Ensuring audit logs contain the following events:

2.17.1.1. System Access;

2.17.1.2. Alterations to user account rights and permissions;

2.17.1.3. System security logs;

2.17.1.4. Privileged functions; and

2.17.1.5. Other system owner identified events.

2.17.2. Reviewing and updating the list of auditable events on an annual basis;

2.17.3. Ensuring audit records that are able to identify the following:

2.17.3.1. Type of event;

2.17.3.2. Date and time of event;

2.17.3.3. Location of event;

2.17.3.4. Source of event;

2.17.3.5. Success or failure of event (if applicable); and

2.17.3.6. User or subject associated with the event.

2.17.4. Maintaining a storage area for audit records that allows flexibility in the size of information collected;

2.17.5. Providing automatic alerting to system owners for audit processing failures;

2.17.6. Requiring administrators to stop audit record generation if a failure in audit processing occurs;

2.17.7. Reviewing audit records on a monthly basis unless otherwise specified in the audit procedures. Reviews are adjusted as needed depending upon the identification of possible attacks or pain points within information systems. Reports are generated to identify suspicious activity. Data is correlated across different repositories to gain organization-wide situational awareness;

2.17.8. Providing for an audit reduction and report generation capability based on selected event criteria;

2.17.9. Generating time stamps for audit records using the external naval clock time process;

2.17.10. Accessing audit information and tools is limited to those whose job duties require access or the staff members who are performing the audit function;

2.17.11. Maintaining audit records for minimum of six (6) years to meet regulatory requirements; and

2.17.12. Ensuring that information systems can provide audit record generation capability for the auditable events defined in this section.

2.18. Protect removable media by:

2.18.1. Restricting access to raised-floor areas that contain critical network, data backup, and server functions to authorized users, vendors, and customers using automated physical security restrictions and biometrics (where deployed);

2.18.2. Controlling and storing failed or retired hard drives and tape media that contains sensitive information within designated secure areas within facilities using physical control restrictions;

2.18.3. Protecting sensitive information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures;

2.18.4. Protecting and controlling sensitive information media during transport outside of controlled areas using authorized personnel and secured transport;

2.18.5. Maintaining accountability for sensitive information system media during transport outside of controlled areas;

2.18.6. Restricting the activities associated with transport of such media to authorized personnel;

2.18.7. Documenting activities associated with the transport of sensitive information system media;

2.18.8. Employing cryptographic mechanisms to protect the confidentiality and integrity of sensitive information stored on digital media during transport outside of controlled areas; and

2.18.9. Prohibiting the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

2.19. Control access to systems and assets, incorporating the principle of least functionality by:

2.19.1. Ensuring that the respective State system owner approves access to State systems;

2.19.2. Reviewing information system functions, ports, protocols, and/or services are limited where applicable;

2.19.3. Maintaining an enterprise list of software (exceptions, white and black list);

2.19.4. Conducting an annual inventory of systems for any unauthorized software use; and

2.19.5. Removing unauthorized software.

2.20. Protect communication and control networks by:

2.20.1. Approving the flow of information between information systems;

2.20.2. Maintaining usage restrictions, configuration requirements, and implementation guidance for wireless access that;

2.20.2.1. Authorizes wireless access connections by the information system owner;

2.20.2.2. Authenticates wireless access users and devices; and

2.20.2.3. Encrypts wireless access.

2.20.3. Maintaining alternate telecommunication services for essential mission and business functions at primary and alternate processing and storage sites.

Back

3. DETECT

3.1. Develop, identify, and manage a baseline of normal operations and procedures for each major information system that:

3.1.1. Establishes a documented, formally reviewed, and agreed-upon set of specifications for the information system or configuration items within the system; and

3.1.2. Conducts configuration reviews on a bi-annual basis or as needed based on changes to the environment of operations.

3.2. Implement network and information system monitoring that:

3.2.1. Employs automated tools to support near real-time analysis of events, with SITSD providing daily review of the audit logs during the workweek;

3.2.2. Monitors inbound and outbound communications for unusual or unauthorized activities or conditions, (SITSD will notify agencies within 24 hours when their portion of the network is involved in any breaches of network security);

3.2.3. Provides near real-time alerts when the following indications of compromise or potential occur:

3.2.3.1. account privilege escalation,

3.2.3.2. authentication,

3.2.3.3. antivirus/antimalware software,

3.2.3.4. user changes,

3.2.3.5. log errors,

3.2.3.6. system failures,

3.2.3.7. and other network failures;

3.2.4. Monitors events in accordance with security incident and event monitoring objectives;

3.2.5. Identifies unauthorized use of information systems;

3.2.6. Deploys monitoring devices to strategically collect organization-determined essential information and at ad hoc locations, to track specific types of transactions of interest to the state;

3.2.7. Heightens the level of monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or the State based on law enforcement information, intelligence information, or other credible sources of information;

3.2.8. Incorporates legal opinion with regard to monitoring activities in accordance with applicable federal and state laws, Executive Orders, directives, policies, or regulations. NOTE: There are no expectations of privacy when using state computing resources unless specifically indicated by law.

3.3. Conduct monitoring of physical access to information systems that:

3.3.1. Includes review of physical access logs monthly; and

3.3.2. Employs real-time physical intrusion alarms and surveillance equipment.

3.4. Establish a continuous monitoring strategy and conduct continuous monitoring of information systems that:

3.4.1. Provides information regarding current gaps in security to appropriate management officials as result of this process;

3.4.2. Defines roles and responsibilities for detection to ensure accountability;

3.4.3. Ensures detection activities comply with all applicable requirements;

3.4.4. Ensures detection activities are tested;

3.4.5. Reviews audit records on a monthly basis unless otherwise specified in the audit procedures;

3.4.6. Adjusts reviews as needed depending upon the identification of possible attacks or pain points within information systems;

3.4.7. Generates reports to identify suspicious activity;

3.4.8. Correlates across different repositories to gain organization-wide situational awareness; and

3.4.9. Continuously improves detection processes.

Back

4. **RESPOND**

4.1. Develop, document, and disseminate an incident response process that:

4.1.1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

4.1.2. Establishes reviews and updates to incident response policy and procedures within two years of last review; and

4.1.3. Incident response will follow the National Incident Management System (NIMS).

4.2. Conduct training of personnel in their incident response roles and responsibilities on an annual basis.

4.3. Conduct tests and/or exercises of the incident response capability annually using designed tabletop and real-life scenarios/exercises to determine the incident response effectiveness and documents the results. These tests may be coordinated with other groups or plans such as Business Continuity, Disaster Recovery, Continuity of Operations, Crisis Communications, Critical Infrastructure, Emergency Action, etc.

4.4. Implement an incident handling capability for security incidents that:

4.4.1. Includes preparation, detection and analysis, containment, eradication, and recovery;

4.4.2. Coordinates incident handling activities with contingency planning activities;

4.4.3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly; and

4.4.4. Employs automated mechanisms to support the incident handling process.

4.5. Track and document information system security incidents.

4.6. Implement an incident reporting requirement of personnel that:

4.6.1. Ensures incidents are reported to the Service Desk within 24 hours of occurrence;

4.6.2. Ensures SITSD reports enterprise security incident information to Executive staff, the Information Technology Managers Council, Information Security Advisory Council, and the Legislative Audit Division on a monthly basis; and

4.6.3. Employs automated mechanisms to assist in the reporting of security incidents.

4.7. Utilize the SITSD Service Desk, SITSD Information Systems Security Office, National Guard, MS-ISAC, Fusion Center and State Risk

Management and Tort Claims Division as an incident response support resource that:

4.7.1. Provides support and assistance for handling incidents; and

4.7.2. Ensures automated mechanisms are employed to increase the availability of incident response related information and support.

4.8. Develop an ISIRT (Information Systems Incident Response Team) Manual that:

4.8.1. Provides a roadmap for implementing its incident response capability;

4.8.2. Describes the structure and organization of the incident response capability;

4.8.3. Provides a high-level approach for how the incident response capability fits into agency processes,

4.8.4. Meets the requirements of mission, size, structure, and functions of the agency;

4.8.5. Defines reportable incidents;

4.8.6. Provides metrics for measuring the incident response capability for the agency;

4.8.7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;

4.8.8. Establishes management review and approval of the ISIRT on a quarterly basis or to address system/organizational changes or problems encountered during implementation, execution, or testing ;

4.8.9. Ensures distribution of updated versions is delivered to ISIRT members; and

4.8.10. Protects the ISIRT from unauthorized disclosure and modification.

Back

5. **RECOVER**

5.1. Develop contingency plans and procedures for each information system that:

5.1.1. Adhere to established contingency planning requirements through the POL-State Government Continuity Program;

5.1.2. Defines essential mission and business functions and associated contingency requirements;

5.1.3. Addresses maintaining essential mission and business functions despite disruption, compromise, or failure;

5.1.4. Addresses eventual, full information system restoration, without deterioration, of the security safeguards originally planned and implemented;

5.1.5. Establishes recovery objectives, restoration priorities, and metrics;

5.1.6. Addresses roles, responsibilities, and assigned individuals with contact information;

5.1.7. Ensures distribution of copies of the contingency plan to key contingency personnel;

5.1.8. Coordinates contingency planning activities with incident handling activities;

5.1.9. Schedules a review of the contingency plan for the information systems annually;

5.1.10. Requires revision of the contingency plan to address changes to State governance, information system, or environment of operation and problems encountered during implementation, execution, or testing;

5.1.11. Ensures communication of contingency plan changes to key contingency personnel occurs;

5.1.12. Requires review and approval by the appropriate agency authorizing official; and

5.1.13. Protects the contingency plan from unauthorized disclosure and modification.

5.2. Conduct appropriate training through the state continuity program and other training opportunities.

5.3. Conduct appropriate contingency plan testing through the state continuity program, agency continuity program, SITSD, and/or other testing programs.

5.4. Maintain an offsite storage site to be in place and used for essential business functions.

5.5. Ensure an alternative processing site is in place and can be used for essential business functions.

5.6. Ensure alternate telecommunication services are available for essential mission and business functions at primary and alternate processing storage sites.

5.7. Conduct backups of user-level and system-level information contained in the information system as defined by the data owner.

5.8. Provide for the recovery and reconstitution of systems, including transaction recovery, to a known state after disruption, compromise, or failure.

Back

F. Implementation

All state agencies will implement the controls identified in this policy within a three to five year timeframe. Agencies will provide status updates on implementation progress to the CIO in July of each year for the prior fiscal year.

IV. Definitions

Refer to the Statewide Information System Policies and Standards Glossary for a list of local definitions.

V. Compliance

Compliance shall be evidenced by implementing the Policy as described above.

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this instrument are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

VI. Enforcement

Policies and standards not developed in accordance with this policy will not be approved as statewide IT policies or standards.

Enforcement for statewide polices and standards developed in accordance with this policy will be defined in each policy, standard or procedure.

If warranted, management shall take appropriate disciplinary action to enforce this Policy, up to and including termination of employment, consistent with current State Policy. The discipline policy can be found in the MOM Policy System (search for: 261). When considering formal disciplinary action, management will consult with their assigned Human Resource Specialist before taking action.

VII. References

A. Legislation

- 2-15-112 MCA Powers and duties of department
- 2-17-505 MCA Policy
- 2-17-512 MCA Duties and Powers of Department Heads
- 2-17-34, MCA – Security Responsibilities of Department
- 2-6-206 MCA Protection and storage of essential records
- 2-17-524 MCA Agency information technology plans – form and content – performance reports.
- Montana Information Technology Act (MITA)

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- SITSD Procedure: IT Policies, Standards, Procedures and White Papers
- Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- POL-Information Security Policy – Appendix A – Baseline Security Controls
- POL-Information Security Policy – Appendix B - Security Roles and Responsibilities
- POL-Information Security Policy – Appendix C – Security Forms and Blocked sites
- POL-Information Security Policy – Appendix D – Security Framework 5 Core crosswalk to NIST

- **Standards, Guidelines**
  - NIST SP800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations
  - NIST Version 1.0 Framework for Improving Critical Infrastructure Cybersecurity